Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Cancelled)

2. (Currently Amended) A method for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the method comprising:

receiving a HTTP request from a subscriber having an established connection over a first communication network coupled to at least one other communication network, ~~said~~ the request including a Universal Resource Locator (URL);

receiving a profile for ~~said~~ the subscriber;

filtering ~~said~~ the request to determine whether ~~said~~ the subscriber is authorized to make ~~said~~ the request based upon ~~said~~ the profile, ~~said~~ the filtering including:

updating a client HTTP request count when ~~said~~ the request for ~~said~~ the URL is a HTTP GET request or a HTTP POST request; and

applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on ~~said~~ the client HTTP request count exceeds a maximum HTTP request frequency;

and

forwarding ~~said~~ the request to ~~said~~ the at least one other communication network when ~~said~~ the subscriber is authorized to make ~~said~~ the request.

3. (Currently Amended) The method of claim 2, wherein ~~said~~ the applying further comprises setting an alarm when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

4. (Currently Amended) The method of claim 3, further comprising sending ~~said~~ the alarm to an Internet Service Provider (ISP) associated with ~~said~~ the subscriber.

5. (Currently Amended) The method of claim 2, wherein ~~said~~ the applying further comprises dropping the data packet containing ~~said~~ the request when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

6. (Currently Amended) The method of claim 2, wherein ~~said~~ the applying further comprises shutting down the account used to access ~~said~~ the first communication network when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

7. (Currently Amended) The method of claim 6, wherein ~~said~~ the applying further comprises disabling HTTP requests for a hold-down period when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

8. (Currently Amended) The method of claim 7, further comprising increasing ~~said~~ the hold-down period each time ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

9. (Currently Amended) The method of claim 8, wherein ~~said~~ the hold-down period increases exponentially each time ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

10-12. (Cancelled)

13. (Currently Amended) A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method to prevent denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the method comprising:

receiving a HTTP request from a subscriber having an established connection over a first communication network coupled to at least one other communication network, ~~said~~ the request including a Universal Resource Locator (URL);

receiving a profile for ~~said~~ the subscriber;

filtering ~~said~~ the request to determine whether ~~said~~ the subscriber is authorized to make ~~said~~ the request based upon ~~said~~ the profile, ~~said~~ the filtering including:

updating a client HTTP request count when ~~said~~ the request for ~~said~~ the URL is a HTTP GET request or a HTTP POST request; and

applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on ~~said~~ the client HTTP request count exceeds a maximum HTTP request frequency;

and

forwarding ~~said~~ the request to ~~said~~ the at least one other communication network when ~~said~~ the subscriber is authorized to make ~~said~~ the request.

14. (Currently Amended) The program storage device of claim 13, wherein ~~said~~ the applying further comprises setting an alarm when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

15. (Currently Amended) The program storage device of claim 14, further comprising sending ~~said~~ the alarm to an Internet Service Provider (ISP) associated with ~~said~~ the subscriber.

16. (Currently Amended) The program storage device of claim 13, wherein ~~said~~ the applying further comprises dropping the data packet containing ~~said~~ the request when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

17. (Currently Amended) The program storage device of claim 13, wherein ~~said~~ the applying further comprises shutting down the account used to access ~~said~~ the first communication network when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

18. (Currently Amended) The program storage device of claim 17, wherein ~~said~~ the applying further comprises disabling HTTP requests for a hold-down period when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

19. (Currently Amended) The program storage device of claim 18, further comprising increasing ~~said~~ the hold-down period each time ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

20. (Currently Amended) The program storage device of claim 19, wherein ~~said~~ the hold-down period increases exponentially each time ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

21-23. (Cancelled)

24. (Currently Amended) An apparatus for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the apparatus comprising:

means for receiving a HTTP request from a subscriber having an established connection over a first communication network coupled to at least one other communication network, ~~said~~ the request including a Universal Resource Locator (URL);

means for receiving a profile for ~~said~~ the subscriber;

means for filtering to determine whether ~~said~~ the subscriber is authorized to make ~~said~~ the request based upon ~~said~~ the profile, ~~said~~ the means for filtering including:

means for updating a client HTTP request count when ~~said~~ the request for ~~said~~ the URL is a HTTP GET request or a HTTP POST request; and

means for applying HTTP server denial of service attack preventative measures when a client HTTP request frequency based on ~~said~~ the client HTTP request count exceeds a maximum HTTP request frequency;

and

means for forwarding ~~said~~ the request to ~~said~~ the at least one other communication network when ~~said~~ the subscriber is authorized to make ~~said~~ the request.

25. (Currently Amended) The apparatus of claim 24, wherein ~~said~~ the means for applying further comprises means for setting an alarm when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

26. (Currently Amended) apparatus of claim 25, further comprising means for sending ~~said~~ the alarm to an Internet Service Provider (ISP) associated with ~~said~~ the subscriber.

27. (Currently Amended) The apparatus of claim 24, wherein ~~said~~ the means for applying further comprises means for dropping the data packet containing ~~said~~ the request when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

28. (Currently Amended) The apparatus of claim 24, wherein ~~said~~ the means for applying further comprises means for shutting down the account used to access ~~said~~ the first communication network when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

29. (Currently Amended) The apparatus of claim 28, wherein ~~said~~ the means for applying further comprises means for disabling HTTP requests for a hold-down period when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

30. (Currently Amended) The apparatus of claim 29, further comprising means for increasing ~~said~~ the hold-down period each time ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

31. (Currently Amended) The apparatus of claim 30, wherein ~~said~~ the hold-down period increases exponentially each time ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

32-35. (Cancelled)

36. (Currently Amended) An apparatus capable of preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, ~~said~~ the apparatus comprising:

a first receiving interface capable of accepting a HTTP request received from a subscriber having an established connection originating from a first communication network, ~~said~~ the request including a Universal Resource Locator (URL);

a profile request generator capable of generating a profile request based upon ~~said~~ the HTTP request;

a first forwarding interface capable of sending ~~said~~ the profile request to an Authentication, Authorization, and Accounting (AAA) server;

a second receiving interface capable of accepting a requested profile;

a filter capable of determining whether ~~said~~ the HTTP request is authorized based upon ~~said~~ the requested profile, ~~said~~ the filter including:

an updater to update a client HTTP request count when ~~said~~ the HTTP request for ~~said~~ the URL is a HTTP GET request or a HTTP POST request; and

a responder to apply HTTP server denial of service attack preventative measures when a client HTTP request frequency based on ~~said~~ the client HTTP request count exceeds a maximum HTTP request frequency;

an authorizer capable of allowing ~~said~~ the HTTP request to be forwarded on at least one other communication network coupled to ~~said~~ the first communication network; and

a second forwarding interface capable of forwarding ~~said~~ the HTTP request on ~~said~~ the at least one other communication network.

37. (Currently Amended) The apparatus of claim 36, wherein ~~said~~ the responder further sets an alarm when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

38. (Currently Amended) The apparatus of claim 37, wherein ~~said~~ the responder sends ~~said~~ the alarm to an Internet Service Provider (ISP) associated with ~~said~~ the subscriber.

39. (Currently Amended) The apparatus of claim 36, wherein ~~said~~ the responder drops the data packet containing ~~said~~ the HTTP request when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

40. (Currently Amended) The apparatus of claim 36, wherein ~~said~~ the responder shuts down the account used to access ~~said~~ the first communication network when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

41. (Currently Amended) The apparatus of claim 40, wherein ~~said~~ the responder disables HTTP requests for a hold-down period when ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

42. (Currently Amended) The apparatus of claim 41, wherein ~~said~~ the responder increases ~~said~~ the hold-down period each time ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

43. (Currently Amended) The apparatus of claim 42, wherein ~~said~~ the responder increases ~~said~~ the hold-down period exponentially each time ~~said~~ the client HTTP request frequency exceeds ~~said~~ the maximum HTTP request frequency.

44-45. (Cancelled)